The Institute for Information Infrastructure Protection is pleased to have this opportunity to share our thoughts with the Federal NITRD program on the Five-Year Strategic Plan. As a consortium of academic institutions, non-profit, and national laboratories, the I3P provides a unique perspective on the Networking and IT R&D agenda.

The N&IT challenges facing the government mirror many of those faced by industry. Both have identity and authentication, intrusion detection, and vulnerability analysis challenges, to name a few. However, the Federal agencies in the NITRD program face other challenges that are unique to government agencies, or have different or additional characteristics when compared to industry. We will briefly discuss three of these in the limited space allowed in this RFI response.

Attribution in cyber space

Attribution, in the N&IT arena, was defined by an IDA report (IDA Paper P-3792, October 2003) as "determining the identity or location of an attacker or an attacker's intermediary." To that we add "even when the intermediary may or may not be a willing participant in the attack" in our I3P white paper on "The role of cyber attack attribution" (see http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf). This is a particularly vexing problem, as no real path towards reliable attribution was included in the various communications protocols used on the Internet. National defense concerns and capabilities aside, the ability to reliably attribute arbitrary Internet traffic to its origin, or some small set of origins, is of increasing interest to the industry as well as to the member agencies of NITRD. However, this capability must be harmonized with the privacy interests of the public from the start. Furthermore, this cannot be left as just a law enforcement challenge since the private sector has interest in it for preventing fraud and the law enforcement agencies around the world cannot possibly handle all of the demand.

While we agree that full attribution may not always be possible or even desirable, we believe that R&D towards the capability of attribution in cyber space should be a high priority of the NITRD. We do not advocate the position of a specific technological or policy solution to address this challenge. Rather, we see the future of attribution in cyber space as a gradual co-evolution of technology, socialization, policy, and law. This multi-disciplinary challenge is one at which both the NITRD and the I3P excel.

Protection of medical information

By necessity of our mobile population, longer life expectancies, and great leaps in medical technology, the medical records and ongoing medical treatments of citizens are increasingly dependent upon cyber space. In the past, this discussion has focused on standardizing medical record formats and the confidentiality of their exchange. However, in the next few years that focus will

likely be replaced by the concerns for the veracity of medical information as well as its protection from unauthorized update. These new concerns are not limited to the traditional medical data at rest or during exchange, but will include such situations as quickly providing personal medical information during a disaster response or the gathering of live medical data via telemetry outside of a medical institution. This live information has the same privacy and accuracy concerns as the traditional medical data but, by its very nature, telemetry data is more vulnerable to interception, disruption, or other interference. Both the NIH and the AHRQ have taken some steps towards these concerns, and we believe that this growing concern deserves much further study from the technology, policy, education, and legal perspectives.

People: the ultimate critical infrastructure

The public and private sector have taken many steps to ensure the reliability and security of everyday activities on both private intranets and the open Internet. The development and application of hundreds of technologies, books of policies and procedures, and many hours of user education have achieved today's level of reliability and security. This limited success is due, in part, to a failure to realize that efforts towards increasing the reliability and security of any system must be focused upon the users of that system – users of systems make the final decision on how to use them. In the current case, this missing realization is that the people using our computer systems and networks are indeed the ultimate critical infrastructure of all public and private organizations. Whether talking about a malicious insider or an under-educated innocent, the everyday decisions made by individuals around the world clearly affect the reliability and security of the systems we all depend on.

This is indeed a very hard problem to address, requiring the interplay of a broad collection of disciplines. However, the actions taken to date have failed to provide the level of reliability and security that will be needed as the world economy grows even more dependent upon cyber space. Well-known private sector concerns about process control systems (including public utilities), supply chains, and the availability and safeguarding of medical information, combined with the innumerable other critical systems inside of private and public institutions, truly makes the case that the people using these systems should be the focus of a strong R&D agenda across all of the member agencies of the NITRD as well as the private sector.

The Institute for Information Infrastructure Protection (The I3P) is a consortium of leading universities, national laboratories and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States. See www.i3p.org for more information.